Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level

Simon Parkin
TU Delft
Delft, The Netherlands
s.e.parkin@tudelft.nl

Kristen Kuhn
Coventry University
Coventry, UK
kristen.kuhn@coventry.ac.uk

Siraj Ahmed Shaikh
Coventry University
Coventry, UK
s.shaikh@coventry.ac.uk

***Abstract*—The motivation for corporate leadership to engage with cyber risks is increasingly clear. Stories can be seen of cyber incidents which have crippled large-scale businesses, potentially for extended periods of time and at significant cost. Our contribution here explores a much under-researched area — perceptions of cybersecurity and cyber risk at the highest levels of an organisation — with the aim of developing a structured, scenario-driven and repeatable exercise for executive decision-makers. We attempt to understand why cyber risk perception is an important concept but equally a challenging one to grasp. We address this by demonstrating an approach to risk articulation, in terms of systematically constructed scenarios, and assess whether this resonates with decision-makers. As part of this, we also attempt to assess cyber-risk decision-makers for their perception of wider business risks and stakeholders.**

***Keywords*—Security management, Decision making, Business continuity, Risk analysis**

I. Introduction

Cyber attacks pose an existential risk to organisations the world over, as acknowledged by the World Economic Forum's Global Risks Report 2020 [1], sitting just below climate change. The past few decades of enterprise digitisation and automation has led to cybersecurity playing a central role to an organisation's status and resilience. As such, this places it firmly within the responsibility of organisational senior leadership [2] in terms of risk management and ownership.

The significant risk posed by cyber attacks has shown to cripple large businesses and their customer bases, for extended periods of time and at significant cost. Examples include the malware incident at Maersk [3] and the ransomware attack on Norsk Hydro [4]. Other recent examples have shut down major hospitals' systems. In 2017, the WannaCry cyber attack resulted in widespread impacts to the UK National Health Service [5]. In June 2020, destabilising and malicious cyber activities were directed against those whose work is critical to the response against the Covid-19 pandemic, including healthcare services, hospitals and research institutes [6].

This paper is concerned with establishing clarity on how executive decision-makers support wider business to respond to cyber attacks. Such incidents are often complex and riddled with uncertainty. What is clear is that managing business risks that arise from cyber attacks demands informed decisions to be made and the executive leadership must be prepared.

This work represents an exploratory study in an under-researched area — perceptions of cybersecurity and cyber risk at the highest levels of an organisation — to develop a structured, scenario-driven and repeatable exercise for executive decision-makers. This effort aims to assess how cybersecurity and cyber risk are perceived at the top level in organisations. This would ensure alignment of cyber risk management decisions (amidst rapid developments in the technologies of networked, IT-supported business infrastructures) with the view from organisation leadership and, by extension, executive decision-makers. As such, this paper sets out to address the following research questions:

- **RQ1:** Does an approach to risk articulation, which is driven by systematically constructed scenarios, effectively capture insights from decision-makers?
- **RQ2:** Do cyber-risk decision-makers perceive whether wider business risks and stakeholders relate to their domain of decisions?

We take inspiration from war games and strategy exercises, which have evolved into a range of useful tools used for military planning, disaster management, emergency preparedness and national resilience. Planning for business risk mitigation arising out of cyber attacks could benefit from instincts and insights drawn from the decision-making process of participants, including risk perception and ownership. The cyber attack scenarios are key here as acknowledged by Haggman [7] who draws out their value for preparing analytical skills in the cybersecurity context:

> *"The further we seek to gaze into the future, the more we have to employ our imaginative rather than our analytical faculties because of the increased uncertainty. [...] futures imagined on a shorter time frame can often be realistic."*

Pushing on the plausibility of the scenarios (including escalations of cyber-related risks) could be a useful dimension to articulate various challenges around mitigating risks from cyber attacks including stakeholder management, ownership, uncertainty and complexity. There is a trade-off to be had in scenarios that could be realistic on the one hand, and if pushed

Workshop on Usable Security and Privacy (USEC) 2021
7 May 2021, Auckland, New Zealand
ISBN 1-891562-73-8
https://dx.doi.org/10.14722/usec.2021.23014
www.ndss-symposium.org

to be more *ahead of the times*, could actually serve to prepare for unchartered territory.

The rest of this paper is organised as follows: Background to the research and related work are discussed in Section II; the methodology and exercise design explained in Section III; and results presented in Section IV. Closing remarks and consideration of future work are found in Section V.

II. Background and Related Work

A. Executive Decision-makers

Where cybersecurity research has investigated high-level decisions about how the security of organisations and systems are managed, it has mainly focused at the level of security managers [8] and not reached the level of executive decision-makers interacting with other functions at the highest level of an organisation. As computer technology and networked systems increasingly become part of normal business operations [9], there are calls for the role of IT (and in turn, cybersecurity) to be recognised as a top-level, board responsibility, given it's nature and that it *"will impact all aspects of a business including strategy, business development, supply chain, staff and customer experience"* [10].

Thus, executive decision-makers of such organisations are the target of this study. In referencing decision-makers, we acknowledge that this can involve a large group of individuals, as a 'board', and potentially external, 'non-executive' directors (who may be part-time) [11]. We consider 'executives' to be those who must make decisions which drive the direction and strategy of an organisation. Also, *"all organisations are different and each board needs to set its own direction and tone for cyber security."* [10]. This includes various governance models which incorporate different types of decision making, e.g., a classic "hierarchical organisation" or a "matrix organisation" reporting to many others.

While executive boards take many forms, this paper focuses on governance-related decisions which involve multiple executive decision-makers of an organisation. Also, we consider that executive decision-makers have a need to address multiple directives at once, e.g., that the organisation is secure while also being able to operate in its primary capacity. This is especially true when breaches and cyber attacks come to public attention – health trusts shutting off their internet connections and working with pen-and-paper during the WannaCry cyber attack [5] is one example of such a decision.

B. Cyber Risk Perception

Organisational leadership faces all kinds of risks, many of which are distinct from the risks those in other roles must consider to reach informed decisions. Top-level decision-making involves complex interactions between leadership teams [11], around 'episodic' decisions and strategic issues. Senior leaders may receive new information from sources including news articles and peers, and delegate the evaluation of tools and technologies to security managers [8]. Risk perception is relevant for organisational leadership because it influences their decision-making. Understanding cyber risk perception – and its challenges – allows for insights into strategic and guiding decisions taken around cybersecurity and cyber incident response. This is the first step in designing a capacity building exercise for decision-makers who work at the interface of senior security management and the executive leadership.

This is not to say that to be able to assess risk correctly, an organisation must first experience an attack, or a simulated attack. There can be testing or 'drills' of security-related continuity plans. However, since organisations must respond to cyber emergencies or crises we consider learning for crisis, and developing preparedness, through simulations. Simulations not only test preparedness, but can also "provide decision makers with experiential learning" [12].

Errors in judgement by decision-makers, often due to incorrect risk perception, lead to a disproportionate response, which can cause mistakes in resource allocation or incident escalation. The design of scenario-based methods to test and challenge cybersecurity decision-making skills [13] typically factors in four elements: overall objectives, scenario injects, observation methods, and evaluation methods. As such, these are an instrument for decision-makers to learn how to act amidst uncertainty in unfamiliar and complex situations, and develop the strategic *"muscle memory to effectively react"* [13].

C. Related Work

The OCTAVE Allegro risk management method includes threat scenario identification [14], to support examination of threats to specific known assets. Threat scenarios may then expand the risk identification process across dimensions that threats outside of the organization's control, such as 'interdependency risks.' We capture interdependent risks using a risk taxonomy and connections to other roles in the organisation and wider ecosystem, with a view to coordinating response and clarifying the role of cybersecurity in addressing risks.

Rhee et al. [15] specifically explore whether top-level managers exhibit an optimistic bias toward their perception of the security risks which relate to their organisation. This is examined through comparison of executives' responses to a closed-question survey, comparing the risks and extent of control that relate to their organisation, to those perceived for business partners and comparable companies. The authors found an appreciation for the interdependence between organisations, where here we explore the relationship between such interdependence to state level, and the types of risk which may prompt risk response activities.

Shreeve et al. [16] studied the decision-making of participants in a tabletop cyber-physical game. The authors identified four structural patterns and two reasoning strategies to risk decision-making (risk-first and opportunity-first). The authors found that their participants were driven less by risk-first approaches which identify an optimal response (as advocated in standards such as NIST-800-53), and more by the responses that a team is capable of enacting within its existing capabilities and how successful those would be. Here we explore the perceived role of different risk classes and actors in achieving acceptable security outcomes to emerging organisational risks.

The Kaspersky Interactive Protection Simulation (KIPS) [17] is a commercial service targeted at increasing awareness of cyber-related risks at higher levels of management (specifically managers of business systems and IT). The offering is

driven by a view that top-level managers in organisations differ in their perspective on cybersecurity risks. Scenario variations focus on training about identified threats to specific sectors, with a focus on how IT security can be managed in a way that does not hamper production facilities. Here we focus on eliciting perspectives on related threats and challenges in coordinating an appropriate strategic response to cyber-related risks across cooperating stakeholders.

III. Methodology

In this section we describe the design of our scenario exercise and study protocol, informed by the understanding of executive security decision-makers as in the previous section.

Executive decision-makers respond more naturally to a *descriptive* perspective on risk (as opposed to a normative description, e.g., costs and probabilities) [18, p. 14]. This has been seen elsewhere as also applying within the security domain [19]. For these reasons we expose participants to *systematically constructed scenarios* which describe events applicable to their level of decision-making (Section III-A). Risk decisions at this level involve dimensions such as *"uncertainty, ignorance, incomplete knowledge, and ambiguity"* [18], where these serve as parameters in the design of the scenarios (Section III-B). The scenarios are designed to encapsulate a complete description of the process of risk taking, which together with participant responses will provide the full view of risk consideration at the executive level, as highlighted by Shapira [18, p. 21]:

- *Definition of risk*, for a specific situation.
- *Attitudes toward risk*: capture tendencies and values.
- *Dealing with risk*: evaluation, choice, and post-decision behavior.

We address the definition of risk in our scenario design (Section III-A), toward eliciting anticipated responses and choices (Section III-B). A survey (see Appendix) captures these elements, and a debrief after the survey offers participants the opportunity to explain their reasoning.

A. Scenario design for executive cyber-risks

One challenge to designing engaging scenarios is maintaining ecological validity [20]. Although participants will know the scenario is not real, efforts can be made to ensure that the scenario is close enough to reality, that participants can consider the scenario as if they were in a real-life situation that the exercise emulates.

We designed a series of scenarios which, when explored in sequence, explore escalation of complexity and ambiguity in a cyber incident for a hypothetical "Company A", as in Table I. Incidents are presented across multiple rounds in the same exercise to reflect escalating risk levels (low, medium, high).

The content of the scenarios is informed by the authors' knowledge of IT systems and processes which real organisations are likely to have in place, and threats which can affect those elements of organisation infrastructure. Known security incidents in recent history informed the design in terms of signalling what may be possible, in effect acting like Haggman's possible near-future cybersecurity event [7].

Scenario design was informed by known cybersecurity incidents which have affected a business. A similar approach has been used elsewhere to study security analysts [21]. Here, we draw on notable events such as the Norsk Hydro ransomware attack [4] (Scenario 1), the Blackbaud system compromise of 2020 which had potential ramifications for many organisations [22] (Scenario 2), and the WannaCry [5] and NotPetya / Maersk [3] attacks (Scenario 3). We manage the elements of a scenario as escalations across specific dimensions according to the risk level associated with the scenario, as in Section III-B. Scenario content loosely follows a structure of incident, response activity, and executive–level imperatives.

The scenarios capture escalation of attack severity through a series of distinct cyber incidents. The benefit of playing through each scenario is exposure to incidents with varying degrees of impact. In terms of impact from cyber risk, this represents an escalation from low to medium to high (Table I). The severity of the cyber risk is primarily represented as the severity of an attack and criticality of the affected system, but as in Table II can escalate by including a more complex mix of affected people and systems. As the scenario escalates, the level of technical complexity and uncertainty then also grows. To note, the latter is not the omission of detail, but the inclusion of factors in a scenario which a security executive is not expected to have immediate knowledge of.

B. Scenario dimensions

Executive risk decision-making is potentially a process that calls on judgement, control, and skills [18]. We then design our scenarios across clear dimensions, along which an executive participant may draw on *judgement calls*, as a professional involved in a management decision-making process and weighing up factors. This is as opposed to 'calling the odds' as in gambling.

Table II illustrates the dimensions which are used to construct the 'recipe' for each of the scenarios we presented to executive cyber-risk managers: Risk externalities; Stakeholder management; Anticipated risks; Areas of uncertainty; Technical areas of complexity, and; Attack classification. Each column in Table II, 'Low' to 'High', describes responses that the authors anticipate for each scenario. In this sense, the exercise is as much about evaluating the scenario design approach as it is evaluating risk perceptions of participants.

1) Anticipated risks: We assess the scenarios for business risks, as per the *Cambridge Taxonomy of Business Risks* [23], which outlines business risks that could be explicitly modelled:

- *Financial* risks, such as economic outlook and variables, market crisis, trading environments, business and competition;
- *Geopolitical* risks, such as national security, corruption & crime, government business policy, change in government, political violence, and interstate conflict;
- *Environmental* risks, such as extreme weather, geophysical, space, climate change, environmental degradation, natural resource deficiency and food security;
- *Social* risks, such as socioeconomic trends, human capital, brand perception, sustainable living, health and disease;

- *Governance* risks, such as non-compliance, litigation, strategic performance, management performance, business model deficiencies, pension management and products & services.

2) Attack classification: We used a real-world scale for cyber attack categorisation as inspiration, specifically, the scale proposed by the UK's National Cyber Security Centre (NCSC) [24]. The risk impact guides our scenario writing in terms of distinguishing across the severity of the scenarios. The six-category scale characterises cyber attacks, from localised incidents affecting individuals or small businesses, escalating up to a national emergency with major consequences. The latter can include possible loss of life. The following scale was shared with participants before they saw the scenarios:

- *Category 1 (National cyber emergency).* Causes sustained disruption of essential services or affects national security, leading to severe economic or social consequences or to loss of life;
- *Category 2 (Highly significant incident).* Has a serious impact on central government, essential services, a large proportion of the population, or the economy;
- *Category 3 (Significant incident).* Has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or essential services;
- *Category 4 (Substantial incident).* Has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government;
- *Category 5 (Moderate incident).* Poses considerable risk to a small or medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government;
- *Category 6 (Localised incident).* Poses considerable risk to an individual, or preliminary indications of cyber activity against a small or medium-sized organisation.

3) Complexity and uncertainty: We include questions for each scenario, where we ask participants to identify areas of complexity and uncertainty. As a simple measure of the response to the design regarding stakeholders (as in Table II), we ask participants to indicate the perceived scope of responsibility for the incident on a scale from private sector to state-owned.

Table II presents our characterisation of scenarios across dimensions of risk impact, the level of stakeholder management needed, anticipated risks, and areas of uncertainty and technical complexity. The characteristics in Table I are distinctly encapsulated in the narrative of the associated scenario. These characteristics become different dimensions over which cyber-risk escalation is expressed. These are self-assessed based on the authors' observations, experience, and analysis of related publicised incidents.

To summarise, the risk externalities (those affected by decisions relating to the risk) [25], stakeholders and anticipated risks are elements directly designed into each scenario. Uncertainty and complexity are introduced in a more subtle fashion. Attack classification is self-assessed based on the author team's interpretation of the NCSC attack categories [24].

C. Study protocol

Each of the three scenario rounds was forty minutes long in duration, to allow participants to read the scenario, ask for clarifications, complete the survey form, and to allow for occasional breaks. For each scenario, the participant group is presented with a summary of the incident designed to evoke a response (as in Table I).

After reading each scenario summary, the participants were asked to rate the impact ('attack classification', Section III-B) and to select and rank the business-related risks which they perceive as being present, using a response sheet (see the Appendix for details of these questions). At the end of the exercise, time was allowed for a group debrief and discussion.

In terms of risk ownership and the responsibility to mitigate risk, participants were also asked to position the split of responsibility between state and private sectors on a Likert scale – at either end of a 6-point scale were state responsibility (1) and private sector (5), with the mid-point representing equally-shared responsibility. In closing each scenario-specific round, participants were also asked to note any areas of uncertainty and particular technical complexity they felt were present in each scenario (where these were free-text questions).

D. Ethics

The study was approved as part of institutional human-facing research review. This includes satisfying ethical obligations ensuring participatory consent, due governance of data collection (including storage, processing, sharing and deletion in compliance with GDPR), digital needs met through secure infrastructure, and following distancing protocols due to COVID-19.

We also addressed the principles of the Menlo Report [26] for ethical research in ICT. This includes question design that did not require sensitive business details to be revealed, and an environment which encouraged participation, while also recognising the busy schedules of participants and the time they contributed to the activity; for instance, we designed data collection and questions to facilitate short answers.

We intended to recruit participants who are highly–experienced, who are then also rare to find and recruit. Difficulty in recruiting security managers at this level has been noted elsewhere, due to their high workload and 'poor reachability' [27]. Participation was voluntary, with participants provided a high-level executive summary of results and reflections. We also ensured no hindrance of fair representation of diversity (in terms of age, disability, race, gender, religion, sexual identity) amongst the participants.

E. Participants

The participants were recruited through a national science academy in a European country. Participants were chief information officers and IT managers, all with some responsibility of decision-making for cyber security in their respective

TABLE I. EXERCISE SCENARIOS. THESE ARE WRITTEN AS A NARRATIVE AROUND AN ORGANISATION REFERRED TO AS "COMPANY A". WHILE PRESENTED AS THREE SCENARIOS, THE PARTICIPANTS ARE OFFERED A CONTINUING NARRATIVE TO START WITH SCENARIO 1 WHICH THEN ESCALATES IN TWO SUBSEQUENT ROUNDS THROUGH SCENARIO 2 AND SCENARIO 3, AS A SERIES OF DEVELOPMENTS.

Scenario 1
The IT Team at Company A has reported a possible ransomware attack on their enterprise server, resulting in the encryption of the company's central data storage. This has caused the company's accounts and finance, and human resources teams to have no access at all to their data. The IT team have shared a communication from alleged hackers asking for a ransom of US$10,000 within three days from the receipt of the email. The hacking group has threatened to post out stored credit card details of the company's customers on a public site, if the ransom is not paid. They have also threatened to cause further damage to the company. The legal team, who have the remit to assure Company A's compliance with GDPR, have been asked to assess what liability is there to Company A. The CEO has asked for an immediate investigation of the causes (including practices and behaviours) that may have led to this attack. Whether this attack has any other impact is also to be investigated.
Scenario 2
The Estates Team at Company A has reported a malfunction with the digital building management system (BMS). The BMS is used to control the heating and ventilation of the entire HQ of Company A. This is a new system that has been operational only for the past year, and is critical to the company complying with national guidelines on managing the carbon footprint resulting from energy usage. The malfunction has caused the top floor of all the buildings in the HQ to be unsuitable for working, and staff located on these floors have had to work remotely for the past week. The IT Team has confirmed that the new BMS is connected to the corporate IT network. They have confidently denied any link with the recent ransomware attack. They have asserted that the central data storage, which was the main target of the ransomware attack, has no link to the BMS system even if both are connected to the corporate IT network. The Estates Team have had the suppliers of the BMS investigate the malfunction. The BMS supplier has reported that they have not encountered such a malfunction before, and are not ruling out an intentional malicious attempt for which Company A has to take responsibility. The suppliers have argued their technology is in use all over the world for several years insisting their technology is reliable. The above has raised tension between the IT and Estates Teams, as the possibility of this being linked to the recent ransomware attack has not gone away. The CEO has asked for the health and well-being of the staff affected in the relevant areas to be prioritised, along with a wider investigation.
Scenario 3
The national media is reporting a nation-wide cyber attack on the country's infrastructure, targeting commercial and residential housing, and even infrastructure (including train stations and airport), around the country. The attack is affecting power supply to many of these buildings, directly affecting heating and ventilation systems, access control, and elevators and escalators. Stations and airports have been put on high alert, with many journeys disrupted due to cancellations. A few days before the national incident (above), the national cyber security agency had approached Company A with a view to conducting a forensic examination across some of the computers, corporate network routers and PLCs interfacing the HQ building that was affected previously. The agency staff had confirmed that the impact of the attack on Company A had been a source of further disruption across buildings in other cities; exact details on the resulting impact are not known however. More details on the national cyber attack have been released by the media, which point to a vulnerability in the digital BMS system, supplied by the same supplier to Company A. The vulnerability affects the back-end cloud service provided by the supplier to allow for remote updating of the PLCs. Some of the reports have even pointed a finger to the attack that targeted Company A, calling it the source of the attack. The attack is being attributed to a neighbouring country who has long been an aggressor to its neighbours. While none of this information has been confirmed by the authorities, this has raised concerns amongst the top leadership of Company A. The Board of Directors of Company A are now wanting more details from the IT and Estates Teams. Some of the Directors are wanting to issue a press release to assure the wider public.

organisations. The background of the participants provided a mix of public and private sector organisations. A few of the participants also held advisory roles in government, with responsibility for working closely with the private sector for cyber resilience.

There were 19 participants, with experience of IT-related decision making ranging from 1 to 10+ years. There was one additional attendee who did not complete any of the demographics or per-scenario surveys; they cannot be included in the Results regarding structured questions, but had the potential to contribute to the post-scenario discussion. For simplicity based on their level of participation, we regard this as not having happened.

Participants were asked to indicate their responsibilities in a pre-workshop survey (see Appendix). Responsibilities are diverse, spanning the procurement of new services and equipment, to IT support and policy management. Three participants did not respond to this question, including the attendee who did not complete any surveys.

It was important to capture the nature of participants' existing risk focus, which we also asked about using the Cambridge Risk Taxonomy. This is represented in Figure 1, illustrating a focus on Technology risks as relating strongly to cybersecurity. This can be expected, although the perceived importance differs, as indicated by the number of different rankings/colours on this particular stacked bar. There is also recognition here of Governance and Financial risks as being strongly related to cybersecurity in organisations; participants recognised the relevance of other risks (see Section III-B).

IV. RESULTS

Two of the authors facilitated the workshop with participants. Here we discuss participant responses to the scenarios in initial subsections, as recorded in survey answers, and as also derived from overview notes taken by the authors facilitating the workshop (as in Section IV-E). We refer to Scenario 1, Scenario 2, and Scenario 3 as S1, S2, and S3 respectively.

A. Pre-scenario risk ranking

We saw – as in Figure 1 – that all of the six categories were ranked by the participant group, although where they

TABLE II. SCENARIO DIMENSIONS. EACH DIMENSION, OR CHARACTERISATION, IS REPRESENTED IN EACH SCENARIO. THE CHARACTERISATIONS REPRESENT A MIX OF ELEMENTS DESIGNED INTO EACH SCENARIO, AND ANTICIPATED RESPONSES WHICH WOULD BE WITHIN EXPECTATIONS WHEN ENGAGING WITH PARTICIPANTS.

Characterisation	**Scenario 1 (Low)**	**Scenario 2 (Medium)**	**Scenario 3 (High)**
Risk Externalities (in terms of who and what is directly and evidently affected beyond the IT Team)	**Who?** Customers **What?** Customer Data	**Who?** Company Staff Other Building Occupants Estates Team **What?** Access to physical space Access to dependant services Building control Staff health and well-being	**Who?** Company Staff Other Building Occupants Estates Team Residents (across cities) Commercial occupants (across cities) Infrastructure Owners/operators (Stations/Airports) Relevant (public) agencies **What?** Access to physical space Access to dependant services Building control Building maintenance due to non-access
Stakeholder Management (Internal / External)	Senior Management (Int.) Legal Team (Int.) Customers (Ext.) ICO (Ext.)	Senior Management (Int.) Legal Team (Int.) Estates Team (Int.) Staff (Int.) (in terms of health and well-being) BMS Supplier (Ext.)	Senior Management (Int.) Legal Team (Int.) Estates Team (Int.) BMS Supplier (Ext.) National Cyber Security Agency (Ext.) Public (Ext.) (in terms of any PR/media engagement)
Anticipated Risks (in terms of Cambridge Business Risks (Family/Class)) (Number of Risk Families Exposed)	Technology/Cyber Governance/Non-compliance /Negligence Social/Brand Perception /Negative Customer Experience	Technology/Cyber Governance/Non-compliance/Negligence Governance/Non-compliance/Occupational Health and Safety Social/Human Capital/Labour Disputes & Strikes Social/Brand Perception/Negative Media Coverage Financial/Counterparty/Supplier Failure	Technology/Cyber Technology/Critical Infrastructure Governance/Non-compliance/Negligence Governance/Litigation Social/Brand Perception/Negative Media Coverage Geopolitical/Interstate Conflict/Asymmetric Warfare Financial/Counterparty/Supplier Failure
Areas of uncertainty (by design)	Financial liability (owed to customers) Further damage from the ransomware attack	Financial liability (owed to staff, and any other HQ building occupant) Further damage from the ransomware attack Further damage to the HQ building	Financial liability (owed to national claimants and BMS supplier) Further damage from the ransomware attack Further damage to the HQ building Further damage across the nation Involvement of an aggressive state actor
Technical areas of complexity	Malware (Ransomware)	Malware (propagation from corporate network to BMS) Digital Building Management Systems (BMS) (Network Interface)	Malware (propagation from BMS to backend cloud system) Digital Building Management Systems (BMS) (PLCs + Remote Updating) Digital forensic examination
Attack Classification	5 (Moderate incident)	3 (Significant incident)	1 (National cyber emergency)

appeared in the ranking differed. As might be expected, where Technology was ranked by our participants, a 1st-place ranking appeared more here than for any other category, and relatively high up the list (no participants ranked it 5th or 6th). No participants ranked Environmental risks in 1st place, but interestingly at least two or more participants ranked every other category as the most important risk to an organisation before seeing our scenarios.

B. Scenario attack categorisation

As in Figure 2, participants noted a shift in the general severity of the scenarios as the complexity and severity increased (Table II). This was certainly the case from S2 ('Medium') to S3 ('High'), if not S1 to S2. This indicates that the design of increasing severity through 'medium' may require attention to articulate an intermediate set of circumstances. The radar chart shows how the categorisation selection was spread across participants – even in our limited cohort, there was then some convergence but not absolute agreement on how to categorise incidents.

C. Scenario risk categorisation

We saw that the diversity of indicated risk categories increased as the scenarios became more complex, represented simply as the average number of risk categories selected by participants for each scenario (participants could select one or more). For S1 the average is 2.68; S2, 2.84, and; S3, 3.63.

Looking at Figure 3, Financial risk was seen as the 'top' risk for S1, Technology for S2, and Geopolitical for S3. Within expectations, S3 shows a greater divergence of categories being selected than S2 and certainly in comparison to S1 (the 'complexity' of the risk landscape was seen by participants to have broadened).

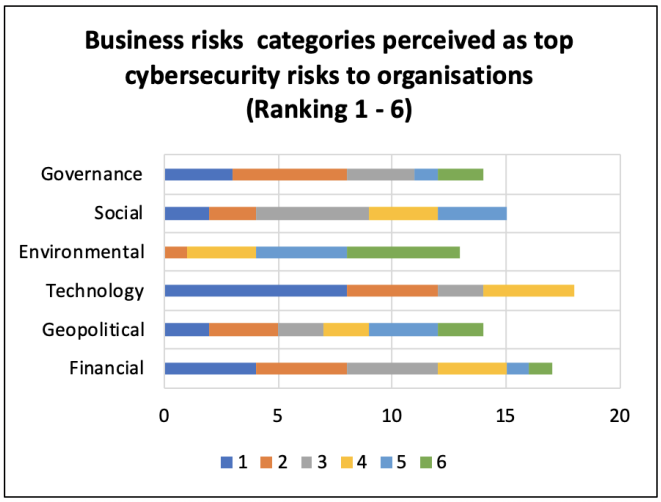

Fig. 1. Top perceived cybersecurity risk categories, from the pre-workshop survey (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking.

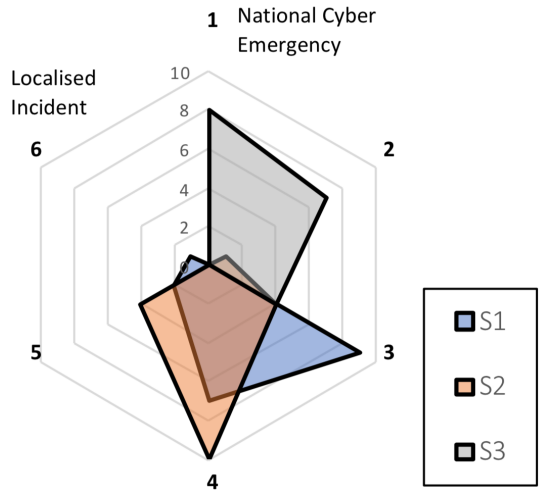

Fig. 2. Radar chart showing number of selections by participants of each attack category (across the 'spokes' of the chart), against the six vertices of the diagram. Each vertex represents one of the six defined 'attack classification' categories, category 6 for a localised or emergent incident, and category 1 for a much more severe, national cyber emergency.

No one risk category was completely ignored, though we may regard Environmental (for S1) and Geopolitical (S2) as having been categorised as non-critical risks. For each scenario, there were categories which were ranked differently by different participants (e.g., Financial in S1, Social and Technology in S2, and Social and Technology in S3). That is, a factor was seen as important, but opinions on *how* important it was differed, in some cases across the entire ranking scale.

D. Responsibility mix

Participants were asked to indicate their perception of the private-public mix of responsibility for risks seen in each scenario (Figure 4), on a scale of 5 (Private sector) to 1 (Public / State). Values around the centre of the scale indicate shared responsibility. Figure 4 shows a transition akin to a 'wave' when stepping through the scenarios, marginal from S1 to S2, and pronounced from S2 to S3. Participant responses for free-text questions support this, e.g., P7 (for S3), remarking rhetorically that the state should *"support the investigation"*. It is interesting to note that the range for each scenario is within two steps on the scale – 5–3 for both S1 and S2, and 4–2 for S3, with a slight shift of perceived responsibility toward the State in S2 compared to S1. No participants perceived any one scenario as being the sole responsibility of the State.

E. Reflections on uncertainty and technical complexity

The workshop included a dedicated debrief and discussion section, where participants were able to raise any points or clarifications about their thought process when responding to each scenario. At the end of each round, participants were asked to comment on uncertainty and technical complexity, from which the quoted comments are derived. We report on our findings along with some of the related areas addressed in an open discussion that followed each scenario assessment.

1) Scenario 1: Participants observed that the scope and impact of ransomware attacks need validation. Very often there is a knee-jerk response to ransomware (in terms of discussions on whether the ransom is paid, who is behind the attacks, and so on). The implication here is organisations should consider more carefully what existing procedures could be invoked (in terms of backup and recovery options), and how to assess the veracity of the claims being made by perpetrators. Essentially then, ransomware depicts uncertainty in terms of the actual danger it poses, and the need for validation. In response to Q4 (about uncertainty), P8 captured the essence of this when they commented *"The full extent of the damage is not clear. It is uncertain whether there was a breach of internal security protocols and whether someone internal to the company is responsible, intentionally or not"*. Moore et al. [8] note that senior security managers may have a sense that the nature of uncertainty means not all risks can be actively mitigated.

While the scenario was designed to carry a certain level of complexity, several participants expressed the need for more detail to better assess the scenario, with P13 commenting *"More information is needed regarding the segmentation of the networks and backups in order to draw any definitive conclusions"* in response to Q5 (about technical complexity).

2) Scenario 2: The nature of the customer-supplier relationship was a particular point of discussion for Scenario 2. Regarding how much responsibility suppliers carry, this was expressed both in terms of: (i) What support they offer to investigate and recover from serious incidents, and; (ii) How contractual terms with suppliers need to cover for liabilities that customers carry.

In response to Q4 (uncertainty), participants explicitly challenged *"Who is responsible for the resolution of the problem?"* (P1), and *"What is most important to be established is where the actual liability is - with the supplier or with Company A?"* (P8). Nearly a third of the participants raised questions around the exact nature of responsibility carried by the supplier in response to such an incident.

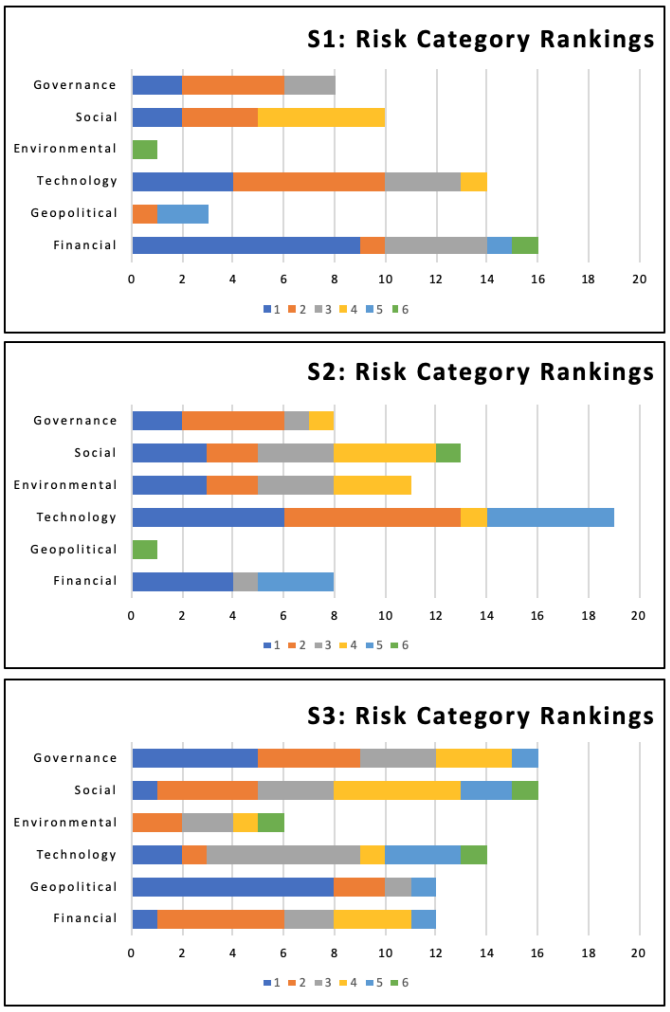

Fig. 3. Business risk category rankings by no. of participants, for each of the three scenarios (1 highest, 6 lowest). The x-axis indicates the total number of participants who have included each category in their ranking.

The nature of escalation in Scenario 2 posed by the introduction of the Building Management System (BMS) also raised the level of perceived complexity, as noted by a quarter of participants. In response to Q5 (complexity) comments ranged from the exact nature of the connection between the corporate network and the BMS, and the nature of potentially unique vulnerabilities carried by systems such as the BMS.

3) Scenario 3: The participants highlighted the responsibility split between state and private sectors, within the context of a major incident. The role of national agencies, and organisational responsibility to wider national stakeholders was also questioned. This was set in the context of different national policy frameworks and ecosystems. The participants' shift to state taking responsibility for this incident is clear from Figure 4; governance and social risks were seen as of importance to a majority of the participants, but with varying levels of priority associated with it.

The shift to the state for responsibility was summed up by two of the participants, who made this explicit: *"If there is a national threat, shouldn't the state support the investigation?"*

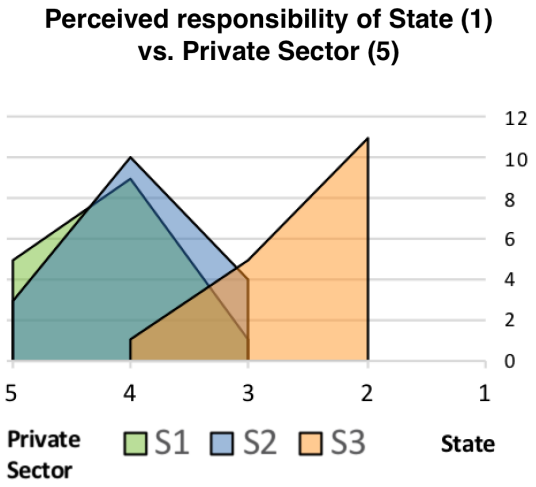

Fig. 4. Tally of participant perception of the responsibility of the organisation ('private sector') against that of the state in managing the risks in each scenario (S1–S3). The y-axis indicates number of participants who have selected each of the values 1 ('State') to 5 ('Private Sector').

(P7), and *"In any such situation, there is a need and necessary actions that the state must take with regard to the strategic objects of national security."* (P14). Moore et al. [8] note that some senior security managers in some organisations may also be proactively briefed by the state about emerging threats.

The range of complexities posed by this scenario were captured, where some of the key themes touched upon by the participants include the *"attribution to neighbouring states"*, sector-specific inter-dependencies, *"cascading effects"* from cyber attacks, a need for greater communication between agencies and private sector, and *"technology support for [public limited companies]"*.

V. Discussion & Conclusion

Here we reflect on both the design of the scenarios, and the responses of participants to the scenarios, as emerged during the exercise itself and the associated data collection.

A. Scenario design and perception of risks

In terms of methodology (RQ1), our use of attack categorisation [24] and risk categorisation [23] provides guidance on the design of scenario escalation. These mechanisms allow for the use of narrative hints on the nature of associated risk, stakeholders involved, and non-technical complexities. Such categorisation is also employed as a means of assessment. This underlies a structure to the scenarios as a novel approach to capturing responses, providing potential for benchmarking across groups and sectors (as seen elsewhere in the development of tabletop cybersecurity games [28]).

The participants in this study were briefed on the risk categories from the *Cambridge Taxonomy of Business Risks* [23] before the scenario assessment to make explicit the scope of risks for the study. As such, the taxonomy offers a particular value for structured understanding of business risks, factoring in societal, environmental and geopolitical risks as above and beyond risks internal to the organisation. Future work

would employ the taxonomy to probe the participants for prior awareness and direct handling of various risks. This would inform the confidence which can be placed in their understanding and perception of risks in response to complex organisational scenarios.

Another opportunity building on the use of the *Cambridge Taxonomy of Business Risks* is to derive meaningful metrics that factor in executive cybersecurity decision-making. This could include whether certain risks such as *social* risks may push up liability concerns, or *geopolitical* risks that may imply state intervention of some form. Any such business concerns could aid executives in identifying non–technical solutions, such as cyber–insurance or outsourced mitigation, for example.

Executive decision-makers must be prepared to address cyber risk perception, as is increasingly evident. The work presented here investigates cyber risk perceptions at the highest levels of organisations. In essence, there needs to be a means to raise awareness and aid learning, so that these decision-makers are prepared to take the appropriate decisions when cybersecurity-related incidents occur.

Our focus on risk perception and ownership, rather than risk mitigation, is an acknowledgement that at an executive level decisions are primarily directed at strategy and resource management. Most actual mitigation typically sits at a layer below the executive, with responsibility for coordination, operations and procedural compliance within the organisation [29].

While acknowledging the complex nature of cyber risk, our scenario design attempted to capture how an incident may escalate across a number of dimensions, and as such how associated risks rise (both in scope and severity). Our findings show that risks were selected within our expectations, and while the perceived private–public risk ownership and risk categorisation broadly overlapped for the first two scenarios, there was a notable shift in perceived risk to a higher level of severity for the third scenario.

In reflection, the narrative in the first two scenarios has a sharp focus on the organisation (that is, the fictional 'Company A') including bearing the impact of the incidents, whereas the third scenario escalates the impact to national infrastructure as part of a *"national cyber attack"*. In sum, our methodology highlights promise in further exploring risk perception from a descriptive risk perspective [18], as opposed to normative perspective (as relates to probabilities, etc.), especially when engaging with risk-related skills and experience.

Regarding RQ2, repeating the study with other groups would serve to validate the pattern of shifts in participants' assessment of the scenarios as they escalate. Equally, this raises the question of whether a "Medium" risk category has sufficient meaning. That there is complexity in the scenario is itself an element of the assessment of risks; the complexity in our scenarios results also from changes across several parameters which act as dimensions to the scenario (such as affected stakeholders, and areas of uncertainty, as in Table II). As noted earlier, the average number of risk categories selected rose only from 2.68 (in S1) to 2.84 (in S2), in contrast with 3.63 (in S3). The jump in *governance* and *social* risks from S1–S2 to S3 is also notable (Figure 3).

B. Future directions

Another lesson to draw here relates to the process of scenario writing. Aside from any organisational dynamics and technicalities of cyber attacks form the content, the perception of risk may also be informed by the choice of terminology for use in the research exercise [30], and nuances hiding in the narrative. This is more of a challenge to tease out, as each participant is informed by their own awareness and experience (where we had acted to 'baseline' this in the pre-survey, to then compare to the scenario-specific responses from participants). There is then a challenge in maintaining ecological validity in the scenarios, in such a way that scenarios resonate with all participants – future applications of the approach will involve consultation with knowledgeable (non-participant) experts to assess scenario content for particular participant cohorts.

In terms of scenario content, aspects of organisational behaviour, such as media attention or dependence on suppliers, may be more tangible dimensions along which to escalate scenarios. As such, these notions may allow for calibration of participants' skills and experience against expected identification of risks, where accounting for the biases of the decision-makers is key in objectively managing business risks [31].

Regarding how executives 'deal with risk' [18], the acknowledgement of various risk types by security executives paradoxically highlights that cyber-risk management in organisations is not the sole responsibility of individual managers. 'Distributed decision making' by security analysts has been observed elsewhere [21]; decisions at the executive level may further involve two-way sharing of information so that the objectives of security and top management are both met. Cyber-risk management is also not an activity to be pursued unilaterally by individual organisations (as indicated elsewhere [8], where security features in perspectives on general business risks [32]). It is a limitation that we engaged only with cyber-risk managers, which will be addressed in future work by involving a range of stakeholders in similar exercises – cyber-related decisions are not only about 'cyber', requiring coordination with others within and outside of the organisation.

ACKNOWLEDGEMENTS

This research was supported by the UK National Cyber Security Centre (NCSC) and Lloyds Register Foundation (LRF) under the "Cyber Readiness for Boards (CRfB)" project.

REFERENCES

[1] World Economic Forum, "The Global Risks Report 2020," 2020, https://www.weforum.org/reports/the-global-risks-report-2020.

[2] National Cyber Security Centre, "Cyber Security Toolkit for Boards 2019," 2019, available from https://www.ncsc.gov.uk/collection/board-toolkit.

[3] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," 2018, available from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[4] K. Fiveash, "The Norsk Hydro cyber attack is about money, not war," 2019, available from https://www.wired.co.uk/article/norsk-hydro-cyber-attack.

[5] A. Morse, "Investigation: Wannacry cyber attack and the nhs," *Report by the National Audit Office. Accessed*, vol. 1, 2018.

[6] North Atlantic Treaty Organization, "Statement by the north atlantic council concerning malicious cyber activities," 2020. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_176136.htm

[7] T. Stevens, A. Ertan, K. Floyd, and P. Pernik, Eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. NATO Cooperative Cyber Defence Centre of Excellence, 2021.

[8] T. Moore, S. Dynes, and F. R. Chang, "Identifying how firms manage cybersecurity investment," *Workshop on the Economics of Information Security (WEIS)*, 2016.

[9] F. Pallas, "Information security inside organizations-a positive model and some normative arguments based on new institutional economics," *Available at SSRN 1471801*, 2009.

[10] R. Horne, "Governing cyber security risk: It's time to take it seriously: Seven principles for Boards and Investors," 2017. [Online]. Available: https://www.pwc.co.uk/cyber-security/assets/governing-cyber-security-risk.pdf

[11] D. Nordberg and R. Booth, "Evaluating the effectiveness of corporate boards," *Corporate Governance: The International Journal of Business in Society*, 2019.

[12] D. Smith and D. Elliott, "Exploring the barriers to learning from crisis: Organizational learning and crisis," *Management Learning*, vol. 38, no. 5, pp. 519–538, 2007.

[13] A. Hussain, K. Kuhn, and S. A. Shaikh, "Games for cybersecurity decision-making," in *HCI in Games - Second International Conference, HCI-Games 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19-24, 2020, Proceedings*, ser. Lecture Notes in Computer Science, X. Fang, Ed., vol. 12211. Springer, 2020, pp. 411–423.

[14] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, Tech. Rep., 2007.

[15] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Computers & Security*, vol. 31, no. 2, pp. 221–232, 2012.

[16] B. Shreeve, J. Hallett, M. Edwards, P. Anthonysamy, S. Frey, and A. Rashid, ""so if mr blue head here clicks the link..." risk thinking in cyber security decision making," *ACM Trans. Priv. Secur.*, vol. 24, no. 1, Nov. 2020. [Online]. Available: https://doi.org/10.1145/3419101

[17] Kaspersky Inc., "Kaspersky Interactive Protection Simulation," 2021, https://media.kaspersky.com/en/business-security/enterprise/KL_SA_KIPS_overview_A4_Eng_web.pdf.

[18] Z. Shapira, *Risk taking: A managerial perspective*. Russell Sage Foundation, 1995.

[19] M. Heidt, J. Gerlach, and P. Buxmann, "A holistic view on organizational it security: The influence of contextual aspects during it security decisions," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[20] S. Schechter, "Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them," *Microsoft, January*, 2013.

[21] A. M'manga, "Designing for cyber security risk-based decision making." Ph.D. dissertation, Bournemouth University, 2020.

[22] L. Kelion, "Blackbaud: Bank details and passwords at risk in giant charities hack," 2020, https://www.bbc.com/news/technology-54370568.

[23] Cambridge Centre for Risk Studies, University of Cambridge, "Cambridge centre for risk studies, 2019; global risk index 2020 executive summary," 2019.

[24] National Cyber Security Centre, "New cyber attack categorisation system to improve uk response to incidents," 2018. [Online]. Available: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents

[25] R. Anderson and T. Moore, "The economics of information security," *science*, vol. 314, no. 5799, pp. 610–613, 2006.

[26] D. Dittrich, E. Kenneally *et al.*, "The menlo report: Ethical principles guiding information and communication technology research," US Department of Homeland Security, Tech. Rep., 2012.

[27] L. Reinfelder, R. Landwirth, and Z. Benenson, "Security managers are not the enemy either," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–7.

[28] B. Shreeve, J. Hallett, M. Edwards, K. M. Ramokapane, R. Atkins, and A. Rashid, "The best laid plans or lack thereof: Security decision-making of different stakeholder groups," *IEEE Transactions on Software Engineering*, pp. 1–1, 2020.

[29] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, p. 101747, 2020.

[30] K. Krol, J. M. Spring, S. Parkin, and M. A. Sasse, "Towards robust experimental design for user studies in security and privacy," in *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*, 2016, pp. 21–31.

[31] D. W. Hubbard and D. Drummond, *How to measure anything*. Wiley Online Library, 2011.

[32] P. Bagri, "The multidimensionality of business risk: A managerial perspective implications for its classification, interpretation & management," 2019.

APPENDIX I – PARTICIPANT-FACING FORMS

Pre-exercise questions

1. What is your current role (job title)? [text box]
2. How many years of work experience do you have? [0,1,2,3,4,5,6,7,8,9,10+]
3. In your current role, who do you report to (given their role/job title)? [text box]
4. Can you give a brief summary of what IT-related decision making do you carry out in your role? [text box]
5. What do you perceive as top cybersecurity risks to organisations? You may choose from any one or more of the following risks: [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. If more than one, could you rank them in the order of priority, with the highest risk at the top (1) down to lower risk at the bottom (6). [Six rows, each with risk labels as above].

Scenario questions (x3 – repeated for each scenario)

1. How would you categorise the current scenario in terms of the following six attack categories? [Cyber Attack categorisation with "category definition" only].
2. Which of the following risks is the organisation in the scenario exposed to in the current scenario? You may choose from any one or more of the following listed in the 'Risks' column below. [Financial, Geopolitical, Technology, Environmental, Social, and Governance]. If more than one, please rank them in the order of priority, with the highest risk at the top (1) down to the lowest risk at the bottom (6). [Six rows, each with risk labels as above].
3. For the purposes of risk mitigation, what is the split of responsibility between the state and the private sector (the organisation in the scenario)? Use the scale below to assign this split between the state and the private sector. Choose '3' if you consider the responsibility to be equally shared between the state and private sector. [5-point scale].
4. From the description of the scenario, what aspects are most uncertain to you? [text box].
5. In terms of technical areas, what areas in the scenario are the most complex to you? [text box].